ISIMC Guidelines for the Secure Use of Cloud Computing V0.10

Presenter Name: Earl Crane,
ISIMC Cloud Security Working Group Chair

Purpose

- **Guidelines provide a framework to help federal departments and agencies make sound, risk based security decisions about how to securely embrace cloud computing.**
- **Assists program managers in deciding what type of cloud model to use for their system from a risk-based security perspective**
- **This paper supports the initiatives identified in FedRAMP efforts for cloud authorization.**

		Cloud Delivery Models		
Cloud Deployment Models		**SAAS (Applications)**	**PAAS (APIs)**	**IAAS (Virtualization)**
	Public Cloud	**Use Case 1: Public SAAS**	**Use Case 2: Public PAAS**	**Use Case 3: Public IAAS**
	Private Cloud (Government Dedicated)	**Use Case 4: Private SAAS**	**Use Case 5: Private PAAS**	**Use Case 6: Private IAAS**

Contributors

Name	Organization
Paul Atwal	Homeland Security
Earl Crane	Homeland Security
Duane Dunston	National Oceanic and Atmospheric Administration
Carlo Espiritu	Health and Human Services
Carrie Gilbert	Department of Justice
Zach Goldstein	National Oceanic and Atmospheric Administration
Keith Hall	Citizenship and Immigration Services
Dr. Emmanuel Hooper	Federal Energy Regulatory Commission
Ronald Johnston	Department of Defense
Toby Levin	Homeland Security
Liz Lyons	Homeland Security
Denise Mallin	Health and Human Services

Name	Organization
Keith McCloskey	Homeland Security
Laura Nielsen	Citizenship and Immigration Services
Matthew Olsen	Social Security Administration
Betsy Proch	Department of Education
Leo Scanlon	National Archives and Records Administration
Roger Seeholzer	Homeland Security
Judith Spencer	General Services Administration
Klint Walker	Department of the Air Force
Robert West	Homeland Security

Advantages, Risks, and Mitigation

- Advantages
  - Efficiency, Cost Saving, Green Computing
- Risks
  - High Risk Threats and Complexity
- Risk Mitigation
  - New Defensive Model
  - Cloud From User, User From Cloud Controls
  - Human To Human, Machine To Machine Controls

Threat

High Risk Threats

- Well-resourced, highly-motivated groups of cyber-warriors
- Both aggressive and pervasive
- Often referred to as the Advanced Persistent Threat in public media

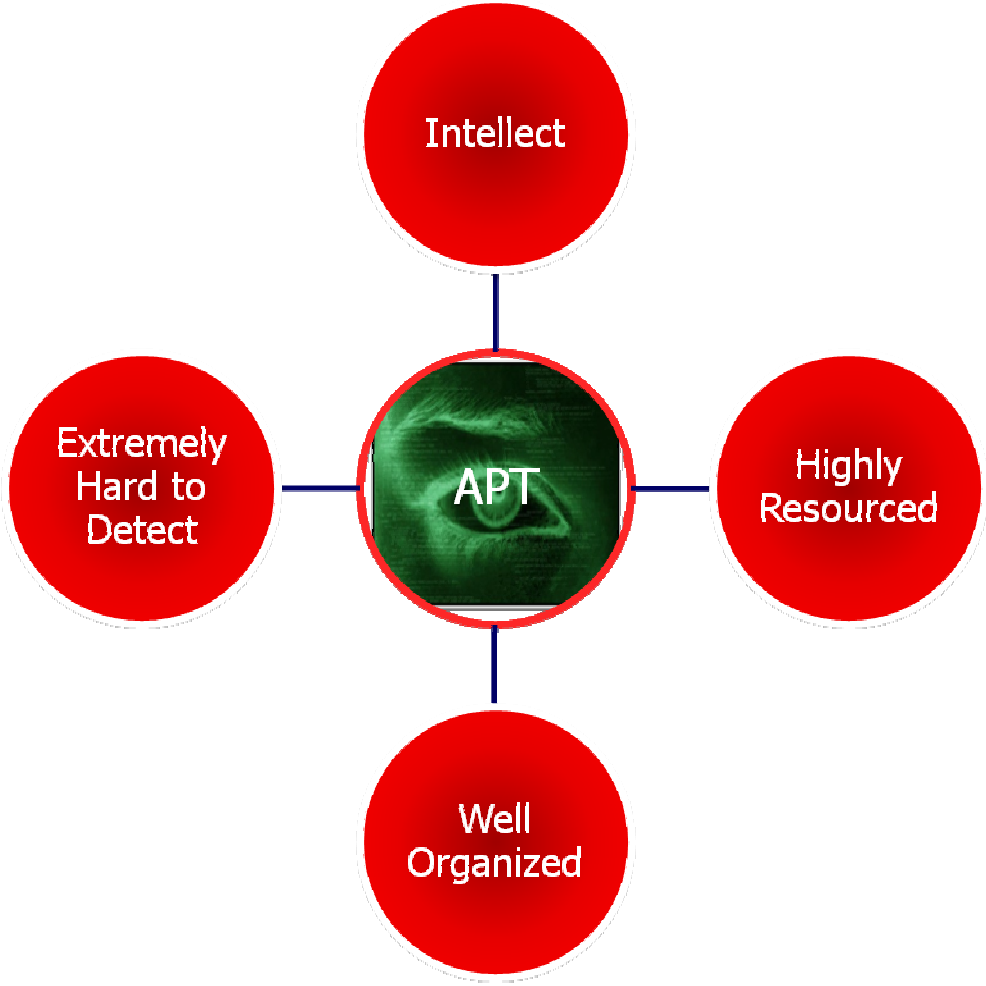
Medium Risk Threats

- Criminals to steal identity and money
- Varying technical sophistication

Low Risk Threats

- Internet Pollution
- Threats against every user

Threat Characteristics



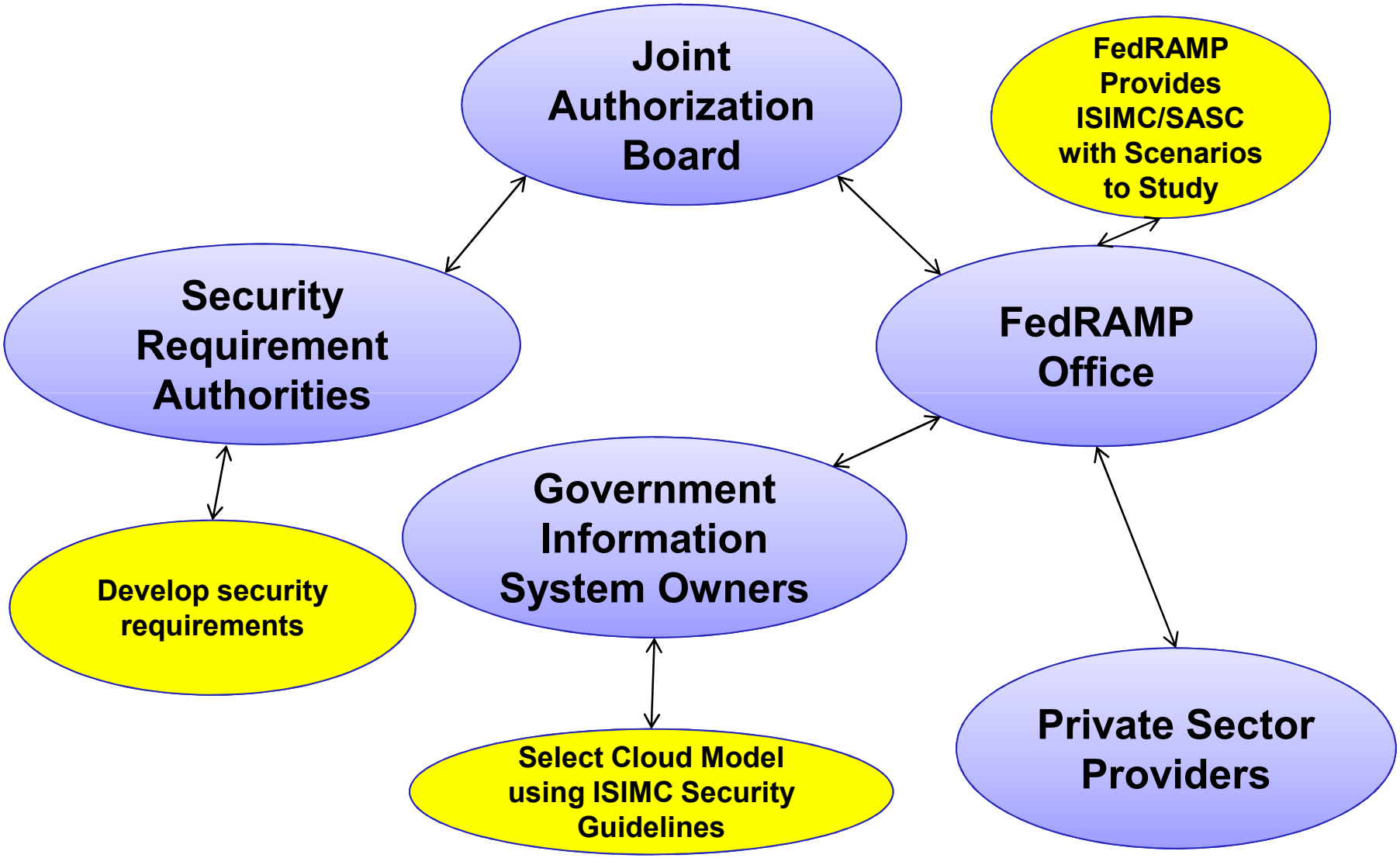
Defensible Approach

- Users From Cloud (UFC) **- Cloud computing environment must have verified, auditable controls in place to provide assurances to the user community that it will not cause them harm**
- Cloud From Users (CFU) **- Cloud environment must be robust and complete in its defensible architecture and controls**
- Machine To Machine (M2M) Controls **- Rapid and automated defense and response, such as malware detection, audit, identification and access controls.**
  - **Do not require any human interaction, can respond in machine-time to detect, respond, and in some cases mitigate threats.**
- Human To Human (H2H) Controls **- Address the intellectual capability of the attacker, and require robust architecture, standardization, risk assessment, policy, and training for human defenders.**
- **A human control will be unable to respond in machine time (H2M), and a machine control will not operate with the sophistication and intelligence necessary to defend against a human attack (M2H).**

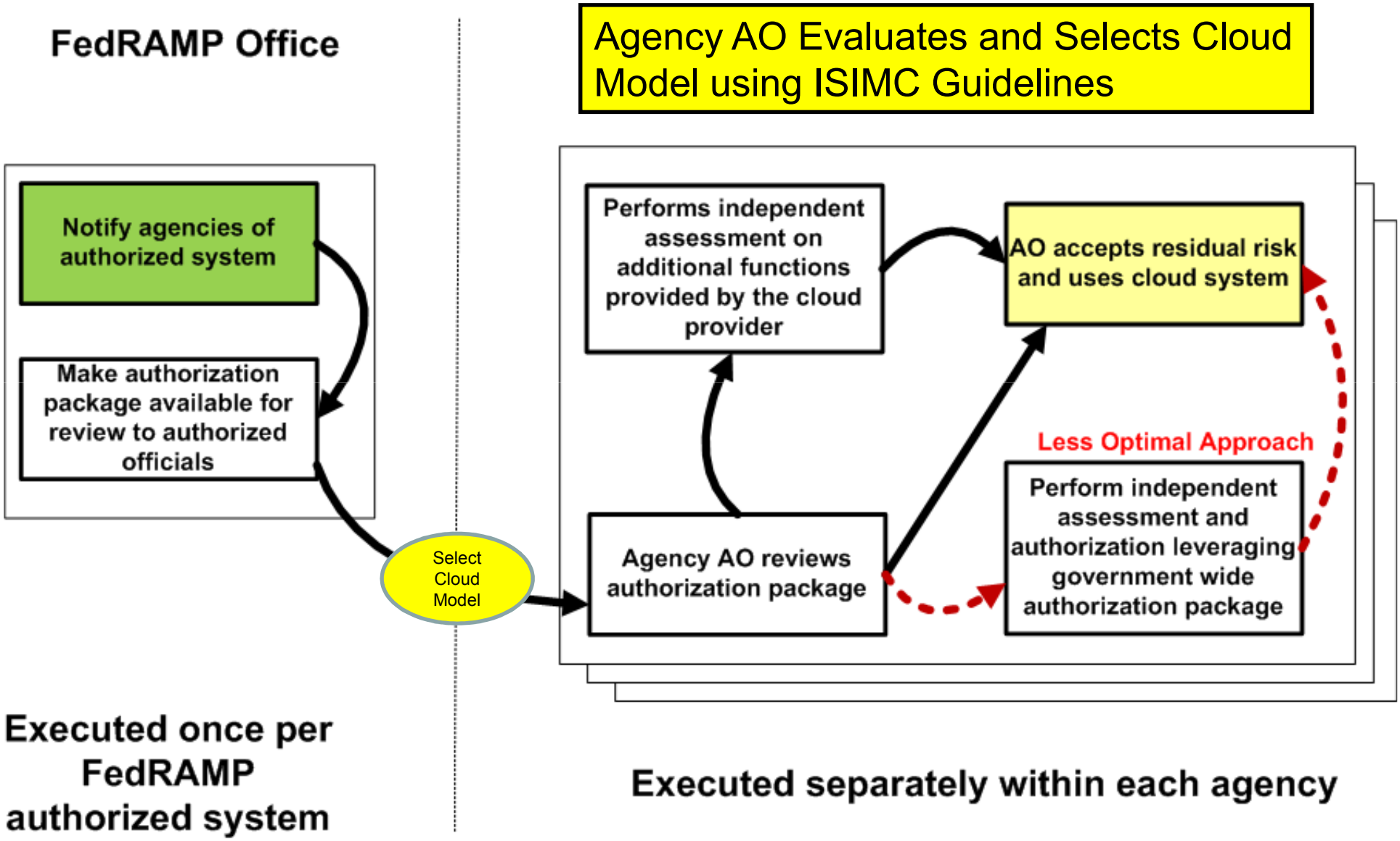
Risk Considerations

- **Control Selection Requires Understanding of:**
  - **Program mission space**
  - **Objectives and requirements**
  - **Operational capabilities**
  - **Can only be made by the program manager**
- **FIPS 199 Categorization as Low, Moderate, High**
  - **Must consider the data's risk posture**
  - **Consider not all clouds will work with all types of data**
- **Service Level Agreements and Contracts**
- **Federal Risk and Authorization Management Program (FedRAMP)**

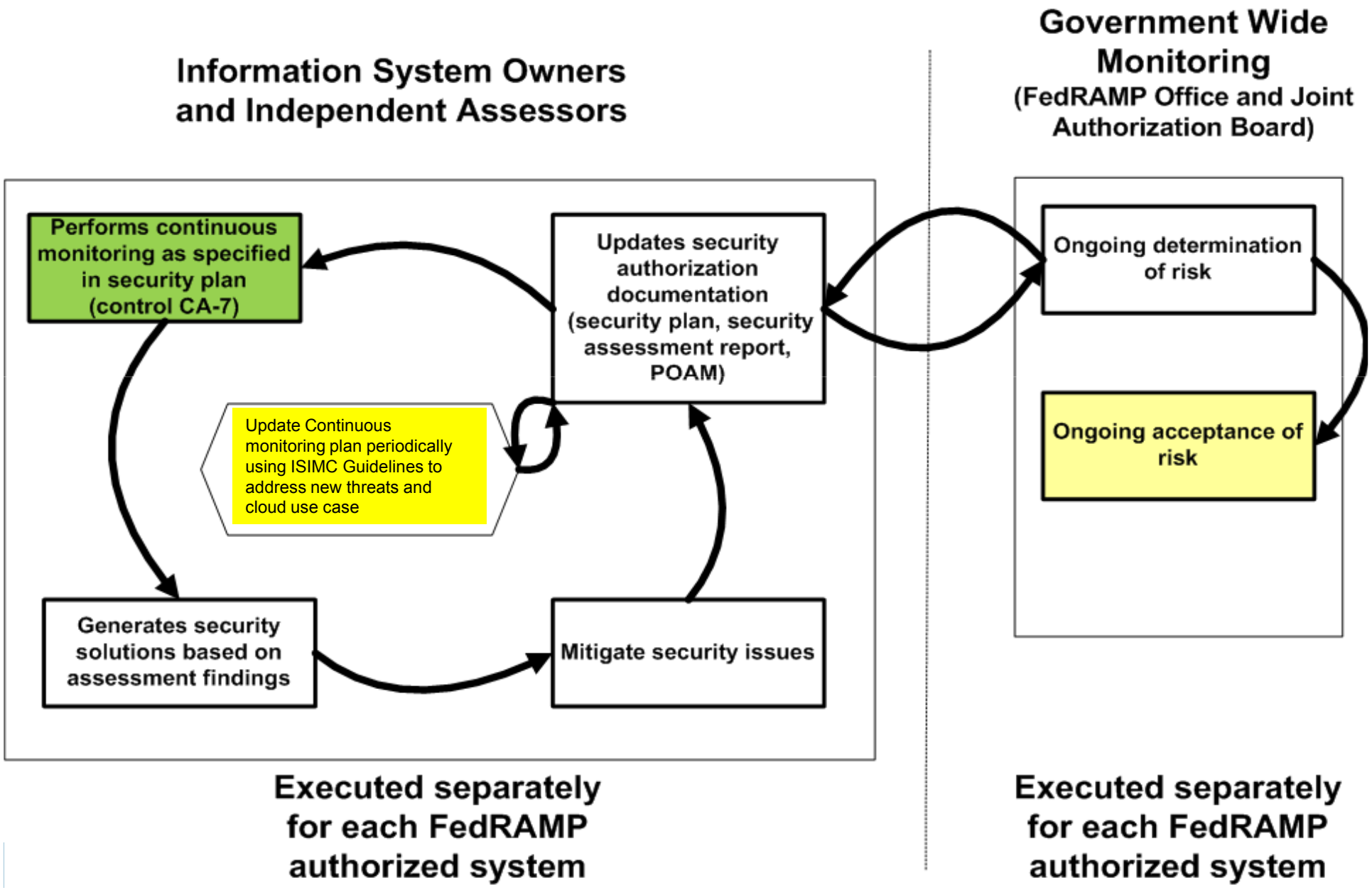
FedRAMP Relationships



FedRAMP Agency Security Authorization Process



FedRAMP Ongoing Risk Management and Continuous Security Monitoring



Six Use Cases

- **Cloud Deployment and Delivery Models have varying security characteristics**
- **Security Capabilities differ based on characteristics**
- **This document helps users select the appropriate cloud model**

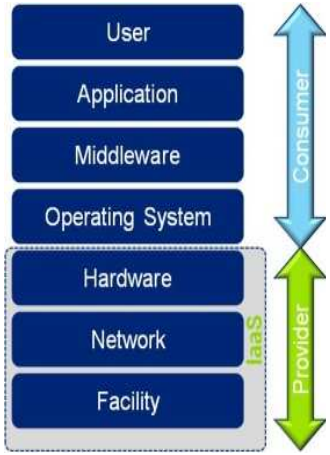
Deployment Model		Service Model		
		SaaS (Applications)	PaaS (APIs)	IaaS (Virtualization)
	Public	Use Case 1: Public SaaS	Use Case 2: Public PaaS	Use Case 3: Public IaaS
	Private (Government Dedicated)	Use Case 4: Private SaaS	Use Case 5: Private PaaS	Use Case 6: Private IaaS

Sixteen Security Domains

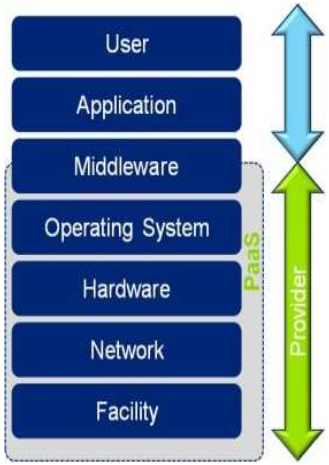
1. Architectural Framework for Government Cloud Computing
2. Encryption, Key Management, and Media Protection
3. Identification, Authentication, and Access Control Management
4. Virtualization and Resource Abstraction
5. Portability and Interoperability
6. Application Security
7. Security Risk Assessment, Authorization, and Management
8. Privacy, Electronic Discovery, and other Legal Issues
9. Contingency Planning
10. Data Center Operations, Maintenance, Configuration, Physical, and Personnel Security
11. Incident Response
12. Compliance, Audit, and Accountability
13. Cloud Lifecycle Management
14. Awareness and Training
15. System and Communication Protection
16. System and Information Integrity

Federal Cloud Security Top 20

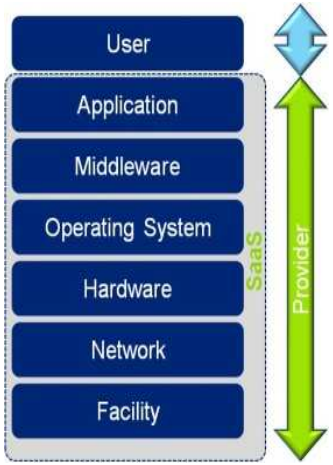
- **Domain 1: Architectural Framework for Government Cloud Computing**
  - **1. Different cloud architectures (SaaS/PaaS/IaaS) have different inherent levels of security visibility and responsibility, the risk environment changes based on the architecture selection, and agencies must take this into account when conducting cloud authorization and control selection. (Domain 1)**



IaaS Stack



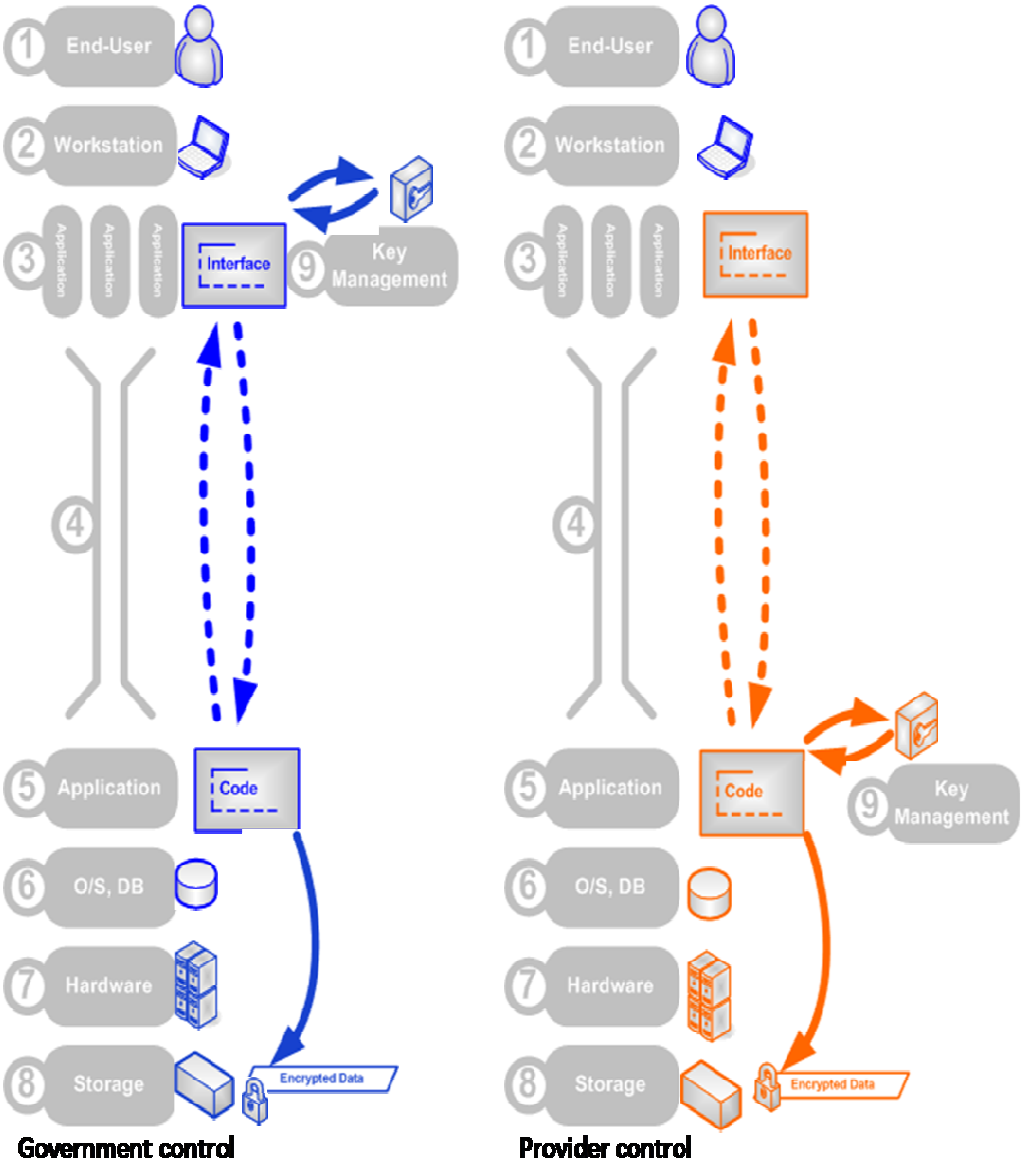
PaaS Stack



SaaS Stack

Federal Cloud Security Top 20

- Domain 2: Encryption, Key Management, and Media Protection
  - 2. Encryption from the data elements to the infrastructure is necessary in a cloud environment to provide confidentiality. Encryption paradigms must shift from system centric to data element centric considerations. (Domain 2)
  - 3. Key management in the cloud environment literally provides the keys to the kingdom – multiple access paths and cloud distribution mean that strong key management in coordination with Identity, Credentialing, and Access Management (ICAM) providers is essential to maintain control over data stored within a cloud environment. (Domain 2)



Federal Cloud Security Top 20

- **Domain 3: Identification, Authentication, and Access Control Management**
  - **4. Promote strong authentication to cloud services, including the use of PIV and PIV-Interoperable, through the use OMB 04-04 *E-Authentication Guidance for Federal Agencies* to determine the appropriate level of ICAM required, and guide ICAM technology selection and implementation using NIST 800-63. (Domain 3)**

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Federal Cloud Security Top 20

- **Domain 4: Virtualization and Resource Abstraction**
  - **5. Virtualization and resource abstraction requires new tools and techniques to maintain visibility, and in some cases improve visibility, for security operators within a virtualized environment. Challenges are specific to the deployed technology, architecture, and Service Models. (Domain 4)**
- **Domain 5: Portability and Interoperability**
  - **6. Cloud portability and interoperability requires the adoption and implementation of standards, and play a unique role in the federal government mission space with mandates to enable information sharing between systems and efficiently use taxpayer resources. The lack of standards results in increased reengineering and additional expense as federal system contracts change cloud vendors. The federal government should establish and/or adopt data and cloud standards to enable cloud portability and interoperability. (Domain 5)**
- **Domain 6: Application Security**
  - **7. Implement and validate application security controls for the cloud environment including code reviews, vulnerability assessments and independent validation. (Domain 6)**

Federal Cloud Security Top 20

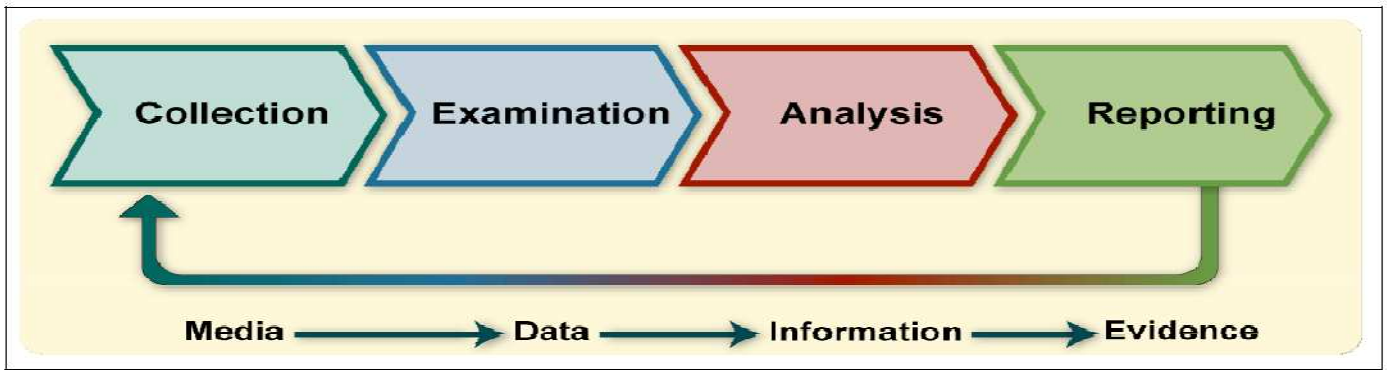
- **Domain 7: Security Risk Assessment, Authorization, and Management**
  - **8. The FedRAMP process is the federal governments risk assessment and authorization baseline for utilizing shared resources such as cloud computing. As such, the FedRAMP process should consider these guidelines for adoption into the risk authorization process, recognizing the identified differences from a traditional system-centric authorization model. (Domain 7)**
- **Domain 8: Privacy, Electronic Discovery, and other Legal Issues**
  - **9. Identify and control the physical location of data and access to the cloud environment for privacy and confidentiality compliance, audit and redress requirements, and breach notification issues. Review contracts, Terms Of Service (TOS), and cloud provider privacy policies to ensure compliance. Conduct Privacy Impact Assessments (PIA) and implement federal privacy requirements such as the Information Practice Principles (FIPPs). (Domain 8)**

Federal Cloud Security Top 20

- **Domain 9: Contingency Planning**
  - **10. Cloud computing does not absolve the agency's responsibility for contingency planning. Agencies must analyze the cloud service provider's contingency plan and SLAs to ensure they meet agency requirements and conduct periodic reviews throughout the lifecycle to address changes in those requirements. (Domain 9)**
  - **11. Contingency planning should recognize that cloud computing is a shared capability as service providers often have more than one agency or customer. This complicates ownership and governance, as multiple customers may rely on the same shared cloud for their contingency planning needs, and exhaust cloud resources during a large-scale event such as a disaster. (Domain 9)**
- **Domain 10: Data Center Operations, Maintenance, Configuration, Physical, and Personnel Security**
  - **12. Recognize that cloud computing exists in a pooled resource environment where compartmentalization may be problematic and traditional government system boundary definitions and inventory identification may require new models. (Domain 10)**
  - **13. Some government-specific mandated security requirements, including least-functionality, personnel security with background and nationality restrictions, and certain NIST security controls may be unfeasible in certain public cloud environments. (Domain 10)**

Federal Cloud Security Top 20

- **Domain 11: Incident Response**
  - **14. Incident response and computer forensics in a cloud environment require fundamentally different tools, techniques, and training for responders to accurately assess a situation and capture appropriate evidence when conducting an incident response that follows federal incident response guidelines. The response plan must address the possibility that incidents, including privacy breaches and classified spills, may impact the cloud and shared cloud customers. (Domain 11)**

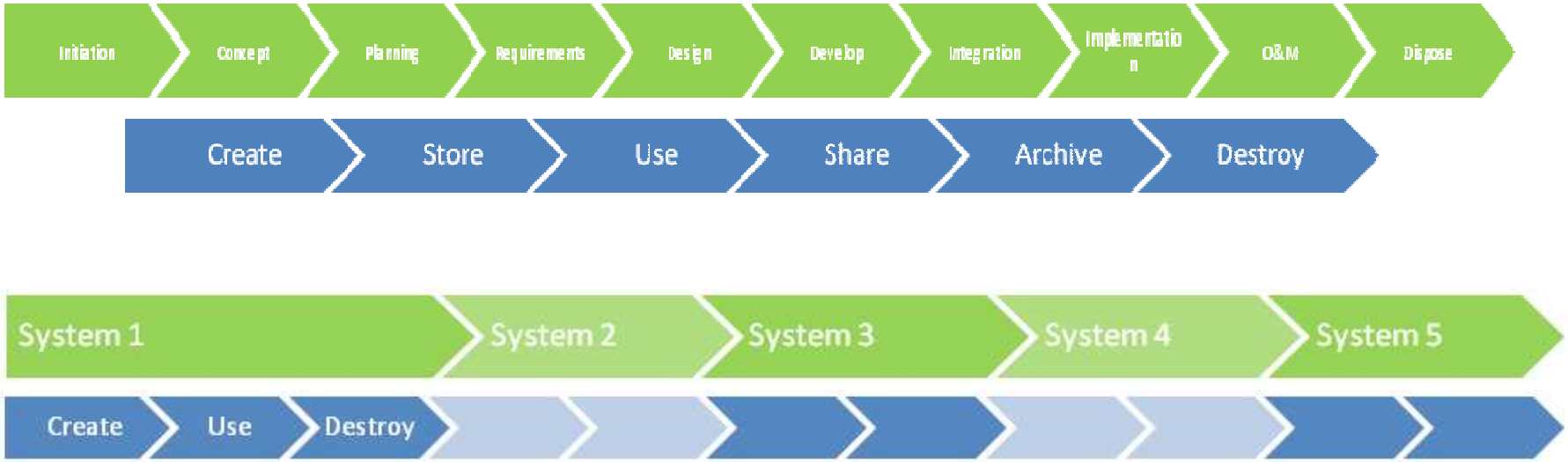


Federal Cloud Security Top 20

- **Domain 12: Compliance, Audit, and Accountability**
  - **15. Compliance with federal laws and departmental policy in a cloud environment requires additional visibility to perform audits, and implementation of robust evaluation criteria as developed by the FedRAMP Joint Authorization Board (JAB) to evaluate cloud security controls. Regardless of the controls, accountability can never be outsourced from the Designated Approving Authority (DAA). (Domain 12)**
  - **16. Cloud computing environments are dynamic and bring new opportunities for real-time audit capabilities, but this requires new continuous monitoring and audit technologies to implement accepted general audit principles. (Domain 12)**

Federal Cloud Security Top 20

- **Domain 13: Cloud Lifecycle Management**
  - **17. While the System Development Life Cycle (SDLC) is important for constructing and managing systems from inception to disposition, use of cloud services require an agency to consider the management of information and the ownership of cloud assets throughout the information lifecycle. (Domain 13)**



Cloud SDLC and Information Lifecycle Management Phases

Federal Cloud Security Top 20

- **Domain 14: Awareness and Training**
  - **18. A Cloud Awareness and Training program should focus on the risks of information disclosure and appropriate system use considering data protection and the cloud FIPS 199 security rating. (Domain 14)**
- **Domain 15: System and Communication Protection**
  - **19. Evaluate cloud compliance with system and communication protection requirements considering compartmentalization, isolation, external and internal connections for system boundaries, routing through Trusted Internet Connections for perimeter protection, and domain integrity requirements such as DNSSEC. (Domain 15)**
- **Domain 16: System and Information Integrity**
  - **20. System integrity in a cloud environment relies on a number of complimentary and compensating controls, from file integrity to malicious code protection to predictable failure prevention. Integrity controls vary at each level of Service Models, as SaaS environments focus on application integrity such as input validation, while IaaS environments focus on file system and data base integrity. (Domain 16)**

Earl.Crane@DHS.gov